Høringsinnspill fra NORWAY CHAPTER OF THE INTERNET SOCIETY (ISOC NORGE)

Høring: Endringer i pengespilloven mv. (DNS-blokkering av nettsteder som tilbyr pengespill som ikke har tillatelse i Norge)
Innspillsdato: 15.01.2024

DNS Blokkering er en fare for Internettet som kritisk infrastruktur

Innledning

Internet Society (ISOC) [1] er en internasjonal og verdensomspennende organisasjon for fremme bruken av og tilliten til internett over hele verden.

Internet Society ble stiftet i 1992 av Vint Cerf [2] og Bob Kahn [3], og blir ansett internasjonalt som en av de viktigste interesseorganisasjonene for Internett, i samme kategori som Internet Corporation for Assigned Names and Numbers (ICANN)[4] og IETF [5].

Internet Society visjon er "The Internet is for everyone". ISOC støtter og fremmer utviklingen av Internett som en global teknisk infrastruktur, en ressurs for å berike menneskers liv og en god kraft i samfunnet. ISOC arbeider for at Internett skal være *åpent, globalt tilkoblet, sikkert og pålitelig.*

NORWAY CHAPTER OF THE INTERNET SOCIETY (ISOC NORGE) jobber for det samme formål i norsk kontekst.

Medlemsstatistikk

- 114,938 Individuelle medlemmer på verdensbasis
- 128 Chapters (avdelinger) and Special Interest Groups (SIGs)
- 82 Organisation Members
- ISOC Norge: 164

Innspill

Både Internet Society (ISOC) og ISOC Norge arbeider for et Internett hvor alle har tilgang til samme informasjon.

Fragmentering av Internettet

Norge har vært en foregangsfigur for et meget viktig kriterium som nettnøytralitet. På samme måte bør Norge arbeide mot enhver fragmentering av Internettet, slik forslaget om DNS-blokkering vil bidra til. Det er uheldig at noen europeiske land allerede har innført blokkering, og dermed har bidratt til et fragmentert Internett samt svekke stadig viktigere sikkerhetsmekanismer for Internett - som DNSSEC.

Sikkerhetsutfordringer ved å svekke tiltroen til sentral infrastruktur

Internet Engineering Task Force (IETF) og ICANN Security and Stability Advisory Committee (SSAC)[6] har i flere rapporter beskrevet tekniske utfordringer og mulige problemer med å blokkere deler av Internettet. Konklusjonen er klar: **Blokkering av Internettet må kun skje dersom en rekke forutsetninger er ivaretatt, men vil uansett gi uheldige innvirkninger på sikkerhet og stabilitet på Internett.**

Referanser:

- RFC7754: https://datatracker.ietf.org/doc/html/rfc7754
- SAC-050: https://itp.cdn.icann.org/en/files/security-and-stability-advisory-committee-ssac-reports/sac-050-en.pdf
- SAC-056: https://itp.cdn.icann.org/en/files/security-and-stability-advisory-committee-ssac-reports/sac-056-en.pdf
- Internet Society Perspectives on Internet Content Blocking: An Overview: https://www.internetsociety.org/resources/doc/2017/internet-content-blocking/

Effektiviteten i DNS-blokkering gitt nye teknologier

A) Blokkering kun virksomt for brukere av norske ISPers DNS-servere

Blokkering vil kun omfatte norske ISPer, og de av deres kunder som bruker ISPens standard navneservere. Brukes alternative DNS-servere eller VPN, vil blokkeringen ikke ha effekt.

B) Bruk av VPN[7]

Bruk av VPN-tjenester har blitt stadig mer vanlig, blant annet som følge av kommersialisering og intens markedsføring av disse i sosiale medier. Verken kostnad eller krav til kompetanse hos bruker er lengre noe vesentlig hinder for bruk av VPN. VPN impliserer også bruk av alternativ DNS-server, og den foreslåtte blokkeringen vil ikke ha effekt.

C) DNS over HTTPS (DoH)[8]

Dette er en relativt ny teknologi for kryptert bruk av DNS-servere, som er i rask utbredelse. Blant annet i Google Chrome, iOS (iPhone)[9] og Android [10] er denne teknologien nå innebygget. Ofte vil brukeren oppleve at DoH er aktivert som en standard innstilling, men selv der dette ikke er tilfelle er terskelen for aktivering dramatisk redusert da all tidligere teknisk kompleksitet ved omgåelse nå er redusert til en av/på-knapp i innstillingsmenyen.

Ved bruk av DoH vil man også bruke en alternativ DNS-server, som Google eller Cloudflare sine offentlig tilgjengelige tjenester.

D) Public DNS Resolvers

Det er meget enkelt for Internettbrukere å endre oppsettet slik at en bruker utenlandske DNS tjenere (public DNS resolvers). Ved å bruke utenlandske DNS tjenere for oppslag, vil en kunne omgå nasjonal DNS blokkering.

En betydelig ulempe med å bruke utenlandske DNS tjenere er at sluttbrukerens DNS oppslag kan samles og brukes på områder som omfatter personvern.

E) Følger for proporsjonalitetsvurderingen

Som beskrevet ovenfor har teknologiutviklingen gjort DNS-blokkering mindre effektivt enn når forslaget først ble fremmet. Proporsjonalitetsvurderingen som diskutert i proposisjonens kap. 5.2., kan derfor antas å være utdatert og ISOC anser det som sannsynlig at en ny proporsjonalitetsvurdering som hensyntar den siste teknologiutviklingen vil kunne resultere i en annen konklusjon.

Noter:

(1) https://www.internetsociety.org
(2) https://en.wikipedia.org/wiki/Vint_Cerf
(3) https://en.wikipedia.org/wiki/Bob_Kahn
(4) https://en.wikipedia.org/wiki/ICANN
(5) https://en.wikipedia.org/wiki/Internet_Engineering_Task_Force
(6) https://www.icann.org/en/ssac
(7) https://codedesign.org/rising-popularity-vpn-what-you-need-know
(8) https://en.wikipedia.org/wiki/DNS_over_HTTPS
(9) https://duo.com/decipher/google-makes-dns-over-https-default-in-chrome
(10) https://security.googleblog.com/2022/07/dns-over-http3-in-android.html

Tilbake til redigering
Send